



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/495,157	01/31/2000	Thomas D. Ashoff	NAIIP075/99.039.01	4471
21186	7590	06/14/2006	EXAMINER	
		SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A. P.O. BOX 2938 MINNEAPOLIS, MN 55402	ARANI, TAGHI T	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 06/14/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/495,157	ASHOFF ET AL.	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 19 October 2005.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-17 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-14, 16 and 17 is/are rejected.

7) Claim(s) 15 is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Taghi, T. Arami
Primary Examiner
Aug 27/81
Taghi Arami
5/19/81

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date .

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. 5/18.

5) Notice of Informal Patent Application (PTO-152)

6) Other: _____.

DETAILED ACTION

1. Claims 1-17 have been examined and are pending.

Claim Rejections - 35 USC § 112

2. Claim 17 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 17 recites the limitation "said firewall" in line 16. There is insufficient antecedent basis for this limitation in the claim.

Response to Arguments

3. As per claims 1, 8 and 17, Applicant's arguments filed 10/19/2005 have been fully considered but they are not persuasive.

Applicant has merely argued that in Grantges reference authorization is made by the gateway 38 and not the firewall 32. Applicant has argued that in Win reference the access menu module 412 is part of access server 106 and not firewall 118. Thus, neither Grantges nor Win describes a firewall.

The Examiner responds that as described in the specification "Firewalls can be packaged as system software, combined hardware and software, and, more recently, dedicated hardware appliances (e.g., embedded in routers, or easy-to-configure integrated hardware and software packages that can run on dedicated platforms), page 2". Grantges discloses in the background (col. 1, lines 59-63) that "one known gateway architecture includes a firewall, a web server, an information collector (IC), an application message router (AMR), and an authorization handler". As also known (Webopedia online encyclopedia

<http://www.webopedia.com/TERM/A/application-gateway.html>) “application proxy or application-level proxy, an application gateway is an application program that runs on a firewall system between two networks”. That is to say, although Grantges’s authorization is made by the application gateway 38 (Fig. 1) on the secure network side of the firewall 32, it is a common knowledge in the art to have the application gateway 38 of Grantges run on the firewall 32 for highly secure method of firewall protection.

Furthermore, claim 17 recites “fourth computer readable program code for enabling the computer system to permit said network resource request through said firewall if said authorization filter is satisfied”. That is, a computer system permits network resource request through the firewall if the authorization is satisfied”. The claim language does not limit the authorization being made by the firewall as argued by the Applicant, rather a computer system, presumably different from the firewall, decides whether to permit the resource request through the firewall. Applicant still has failed to identify specific claim limitations, which would define a patentable distinction over prior arts.

Therefore, the examiner asserts that cited prior art does suggest the subject matter recited in independent Claims 1, 8, and 17 and in subsequent dependent Claims 2-7, and 9-16. Accordingly, rejections for claims 1-17 are respectfully maintained. The Examiner is attempting to clarify the teachings of the prior art reference and how it reads on the claims. In order for the applicant to have ample opportunity to provide perusasive arguments and /or amendment of the claims to overcome the prior art of record this office action is made Non-Final.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-6, 8-13, 15-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grantges (USP 6,324,648) and further in view of Webopedia Computer Dictionary.

As per claims 8 and 17, Grantges and Win teach an authentication method and computer program product at a firewall [Grantges, col. 5, lines 40-57, Check Point One firewall, see also abstract, Figures 1 and 8 and associated texts], comprising the steps of:

- (a) receiving a network resource request from a client user [Grantges, col. 8, lines 15-28];
- (b) querying [Grantges, col. 9, lines 6-18], using a network protocol, at least one directory [Grantges's LDAP] that is configured to store information concerning an entity's organization, wherein said query is based upon an authorization filter [col. 11, lines 13-33, an authorization plug-in 42 queries authorization server containing LDAP server, and determines the application for which access by the user is authorized and builds authentication cookie 90 and application list cookie 92] that is generated based on a directory schema [tree structured LDAP] that is predefined by said entity;
- (c) determining, based on the results of said query, whether the contents of at least part of one or more entries in said at least one directory satisfy said authorization filter

[Grantges, col. 11, lines 15-19, authorization plug-in 42 determines the authorized applications for the user 18]; and

(d) Permitting said network resource request through said firewall if said authorization filter is satisfied [Grantges, col. 11, lines 12-43, the plug-in (42) then through gateway proxy server 40 transmits cookies 90 and 92 to client computer 22].

It is noted (as persuasively argued by the applicant) that Grantges does not explicitly disclose that authorization is made by the firewall. However, it is a common knowledge in the art to have the application gateway 38 of Grantges run on the firewall 32 for highly secure method of firewall protection (Webopedia, definition of application gateway).

As per claim 1, Grantges teaches a system for authorizing client access to a network resource, comprising:

a server [Grantges, col. col. 7, lines 37-44, an authorization server] having at least one directory [LDAP-capable server, light weight directory access protocol] that can be accessed using a network protocol, said at least one directory being configured to store information concerning an entity's organization [Grantges, col. 7, lines 39-44, i.e. X.509 digital certificate, the identification of applications to which access by the user has been authorized by an application trustee, and a gateway user identification(ID)];

and a firewall [Grantges, col. 5, lines 40-57, such as Check Point One firewall] that is configured to intercept network resource requests from a plurality of client users [Grantges, col. 8, lines 15-28], said firewall being operative to authorize a network resource request based upon a comparison of the contents of at least part of one or more entries in said at least one directory to an authorization filter, wherein said authorization filter is generated based on a directory

schema that is predefined by said entity [Grantges, col. 11, lines 12-43, i.e. an authorization plug-in (42) queries authorization server (46) and determines the application for which access by the user is authorized and builds authentication cookie 90 and application list cookie 92. The plug-in (42) then through gateway proxy server 40 transmits cookies 90 and 92 to client computer 22]

As per claim 2 and 9, Grantges teaches the system/method of claims 1 and 8 respectively, wherein said at least one directory is a lightweight directory access protocol directory [Grantges, col. 7, lines 36-37].

As per claim 3 and 10, Grantges teaches the system of claims 1 and 8 respectively, wherein said authorization filter is specified using a graphical user interface [Grantges, col. 11, line 13, authorization plug-in 42].

As per claims 4-5, and 11-12, Grantges teaches system/method of claims 1 and 8 respectively, wherein said authorization filter implements a per-user authentication scheme [Grantges, col. 8, lines 10-11, that is the authentication of the user, see also col. 11, lines 33-34, authentication cookie 90] and, wherein said authorization filter implements a per service authentication scheme [Grantges, col. 8, lines 12-13, see also col. 11, lines 33-34 for application list cookie 92].

As per claims 6 and 13, Grantges teaches the system/method of claims 1 and 8 respectively, wherein said firewall and said directory communicate using secure socket layer communication [Grantges, col. 6, lines 37-42].

As per claim 16, Grantges and win teach the method of claim 8, wherein step (a) comprises the step of receiving a network resource request from a client user at an external

network [Grantges, abstract, authenticating access for a client computer over an insecure, public network to one of a plurality of destination servers on private, secure network].

4. Claims 7 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Grantges as applied to claims 1 and 8 above, and further in view of prior art of record Check Point Management Client, Version 1.0.

As per claim 7 and 14, Grantges fails to teach the system/method of claims 1 and 8 respectively, wherein said firewall is configured to query multiple directories.

Check Point Account Management Client discloses use of an LDAP server containing multiple branches [Page 139].

Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to modify the LDAP server of Grantges and Win with the one disclosed by Check Point for its efficiency and enhanced security [see Check Point, page 13 for the disclosed advantages].

Allowable Subject Matter

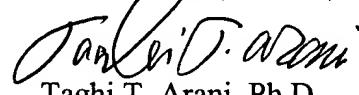
5. Claim 15 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131
5/18/2006